Annex l: Integration of Biometric Authentication

# Authentication Arrangements under the EyeCloud® Platform

The following is a description of the authentication arrangements and responsibilities relating to the authentication of identification and authentication of beneficiaries and is subject in all respects to existing and future agreed Standard Operating Procedures entered into between the Parties.

Collection of biometric data. As part of the registration procedures with UNHCR, UNHCR registers the biometrics for refugees’ and asylum- seekers’ family members above three years of age. Iris scans are stored in a proprietary UNHCR database (aka EyeFSP©) furnished furnished by Iris biometric recognition provider in UNHCR’s regional data centre. The biometric data is linked to the individual identity documentation number of refugees which in turn is linked to the family ID or case ID.

# Integration with EyeCloud ©

The payment solutions will interface with UNHCR’s registration database. The access will be managed through EyeCloud©, which means that beneficiaries will either not need to pre-enroll with the FSP as is the case with the banking payment modality or have a facilitated/digital enrollment in case of mobile wallets onboarding where specific data is fetched from UNHCR for the refugee population. In both cases, the FSP will receive a unique identifier (e.g. the UNHCR individual number) and a cash transfer amount that is associated with that number.

# Authentication

* 1. Under the EyeCloud® architecture, when refugees have their iris scanned at a designated FSP location the information is sent via the FSP’s EyeCloud® Remote Server to UNHCR’s EyeCloud® Host Server through an encrypted virtual private network. The iris scan is performed through a dedicated hardware named EyeCash®. The EyeCloud® Host Server then matches the information with the relevant “individual ID” and returns this information to the EyeCloud® Remote Server. The EyeCloud® architecture may be set up with any licensed FSP. Under the EyeCloud® platform, UNHCR is responsible for identifying and authenticating beneficiaries for receiving cash withdrawals in line with agreed Standard Operating Procedures (SOPs). At the time of authentication, the beneficiary scans his/her eye at the ATMs, agent shops or other designated locations which is then checked against the UNHCR biometric database. Authentication is confirmed or denied. No biometric data is shared for the authentication. The contracted FSP will agree to authenticate beneficiaries by utilizing UNHCR registration data1 with its iris scans as an authentication of identity for the beneficiaries.
	2. The cash assistance delivery infrastructure requires development of a working EyeCloud © platform for authentication, and/or a web-based interface for cash transfer. Minimum technical requirement for the FSP to allow for the integration are following:
* 2G and above network connection
* Windows 10 for the station (64 bi)t and Android for the mobile

1 Iris biometric data has been and will be collected by UNHCR during the registration process and through renewal of asylum seeker certification.

# Responsibilities

* 1. UNHCR is responsible for maintaining the iris database, the EyeCloud® Host Server as well as the links between the FSP virtual account numbers and the refugee biometric and registration data.
	2. UNHCR will also collaborate with Iris biometric recognition provider who will be responsible for the hardware costs (provision of eye-pay devices) for the FSP’s agents and for the deployment of Eye-pay devices at ATM sites etc. UNHCR and Iris biomatric recognition provider will be responsible for all the training costs that may be required in support to FSP staff on hardware and/or software aspects.
	3. The FSP is responsible for creating virtual accounts/ mobile wallets based on the refugee individual numbers, for maintaining the EyeCloud® Remote Server as well as the EyeCloud® integration at the ATM level (such as physical adaptation of the ATM sites, if required, for hosting the eye-pay devices), agents’ network and the larger switch ecosystem. The FSP is furthermore responsible for the reasonable safeguarding of iris-scan equipment /eye-pay devices at each touchpoint once installed.
	4. Both parties, FSP and UNHCR, are equally responsible for ensuring stable site-to-site VPN connectivity between the EyeCloud® Remote Server and the EyeCloud® Host Server. Connectivity problems are to be addressed and resolved immediately and directly between the s a i d t w o parties.